UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,658	03/28/2001	Pascal Paillier	032326-130	2508

21839 7590 04/15/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/818,658	PAILLIER, PASCAL	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 12/22/2004.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-9 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-9 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment, and remarks therein, received on 12/22/2004 have been entered and carefully considered.
2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

3. Applicant's arguments have been carefully considered but they were not found persuasive.
4. A certified copy of the French Priority Application has been located and as a result the rejection referring to this matter is withdrawn.
5. Based on amendments to the and applicant's arguments the examiner withdraws 35 U.S.C. § 101 rejection as pertaining to these claims.
6. Applicant argues that claims 1 and 5 were amended to explicitly recite the application steps in order to clarify the application and overcome the previous Office Action 35 U.S.C. § 112 second rejection.
7. The examiner points out that the clarification of claim 5 is inadequate. Amending claim 5 A introduces more ambiguity. The claim limitation recites: "selecting two integers a, b as candidates". The term "candidates" is not understood as it is not clear what the term refers to. In light of the preamble the term appears to refer to cryptographic keys such as RSA. The previous Office Action pointed out the problem with such an interpretation and applicant did not offer any additional clarification.

8. As per claims 1 applicant argues that "while the Lidl publication discloses that the Carmichael function is known, per se, it does not contain any motivation to combine such as a suggestion that such a function should be used to verify the co-primness of two numbers that are employed to generate cryptographic keys" and summarizes that "there is nothing in the individual disclosures, nor in their combined teachings, which suggests the use of the Carmichael function in a modular exponentiation to verify the co-primeness of two numbers.

9. The examiner points to the previous Office Action *(§ 21)*, wherein motivation to combine verification of co-primness of two numbers that are employed to generate cryptographic keys using the Carmichael function is provided by *Schneier.*

10. Applicant argues that the letter *n* cited by Lidl is not the same as the letter *b* cited by applicant because the letter *b* is the prospective co-prime integer values and not the product of *p* and *q*.

11. The examiner finds applicant's argument non-persuasive. The fact that *a* and *b* are co-prime does not preclude *a* and/or *b* to be a product of two numbers. All it means is that *a* and *b* have no common factor other than 1 and -1, or equivalently, if their greatest common divisor is 1.

12. As per claim 3 applicant states that λ(b) is calculated in advance and stored in memory, and that the rejection of this claim states that theses features are implicit in the equation a^ λ(b) ≡1(mod b).

Applicant provides a counter argument where it is possible to dynamically generate both of the integers and a and b each time a new set of keys is to be generated, wherein the value for λ(b) is calculated each time.

13. The examiner points out that whenever calculation operations occur the data is stored in memory and before a number [a] is multiplied, the number of multiplications [λ(b)] must be known, which reads on λ(b) that is calculated in advance.

14. The notion that the subject matter of claim 7 is not suggested by the references for "similar reasons" is found non-persuasive for *("similar")* reasons *stated* above.

15. Claims 1-9 have been examined.

16. Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

17. The limitation of claim 9: "the portable electronic device of claim 6" is addressed in the preamble of claim 6. The modification to the preamble stands or falls with the claim that recites the preamble. As a result the purpose of the limitation (above) is not understood, and as a result the limitation is assumed to be covered by the art that reads on claim 6.

18. The effective filing date for the subject matter defined in the pending claims in this application is 3/28/2000.

19. Claims 1-6 remain rejected under 35 U.S.C. 103(a) as being unpatentable over Rudolf Lidl and Gunter Pilz ("Applied Abstract Algebra", ISBN 0387961666, 1985; hereinafter Lindl et al.), and further in view of the admitted prior art (AAPA) and Bruce Schneier ("Applied Cryptography, protocols, algorithms, and source code in C",ISBN: 0471128457, 1996) for the reasons discussed in the previous Office Action.

20. Generating at least two cryptographic keys from the integers *a* and *b* when equality is verified is implicit.

21. Claims 6-8 remain rejected under 35 U.S.C. 103(a) as being unpatentable over Rudolf Lidl and Gunter Pilz ("Applied Abstract Algebra", ISBN 0387961666, 1985; hereinafter Lindl et al.) in view of the admitted prior art (AAPA), Bruce Schneier ("Applied Cryptography, protocols, algorithms, and source code in C",ISBN: 0471128457, 1996) and further in view of Murphy et al. (U.S. Patent No. 6226744) for the reasons discussed in the previous Office Action.

22. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rudolf Lidl and Gunter Pilz ("Applied Abstract Algebra", ISBN 0387961666, 1985; hereinafter Lindl et al.) in view of the admitted prior art (AAPA), Bruce Schneier ("Applied Cryptography, protocols, algorithms, and source code in C",ISBN: 0471128457, 1996) and further in view of Murphy et al. (U.S. Patent No. 6226744).

23. Generating a pair of cryptographic keys in the portable electronic device is inherently achieved by utilizing an arithmetic processor and using the

arithmetic processor that verifies the co-primness of integer numbers for generation of a pair of cryptographic keys from these integers would be implicit.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

4/15/05

Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100